13-0579TJS - 13-0584TJS

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT(S)

I, Lyndon George, being duly sworn, depose and state:

I am a Special Agent (SA) with U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), duly appointed to law and acting as such. I have been employed as a Special Agent by HSI since December 8, 2008. I was employed as an Immigration Officer with the Immigration and Naturalization Service and Customs and Border Protection since 1997, prior to joining ICE as an Immigration Enforcement Agent in August 2008. My past and current duties include, but are not limited to the investigation and enforcement of the Immigration and Nationality Act, relating to Title 18 United States Code § 1028 (Document Fraud), Title 18 United States Code § 1546 (Fraud and Misuse of Immigration Documents), and Title 42 United States Code § 408 (Social Security Fraud).

The information set forth below is based upon your affiant's personal observations or upon information provided to me by other law enforcement officers participating in the investigation as indicated. As the purpose of this affidavit is only to establish probable cause, your affiant has not set forth each and every fact known concerning this investigation.

Your affiant submits this affidavit in support of a search warrant to search the residences and vehicles of Antonio Abraham CRUZ-CRUZ, a/k/a "TONY," a/k/a "FDP" (the name of an identity theft victim whose initials are "FDP," and hereinafter be referred to as such) and Henry RAMOS-AGUSTIN for violations of Title 18 United States Code §§ 1028, 1028A, and 1546, and 42 United States Code § 408. Your affiant submits this affidavit in support to search the following:

Owned, Used, or Operated by CRUZ-CRUZ

1) The residence located at 10505 Truxton Road, Basement Apartment, in Adelphi, Maryland 20783;
2) 2000 Gold Chevy Tahoe, with Vehicle Identification Number (VIN): 1GNEK13T5YJ103097, bearing Maryland Motor Vehicle Administration (MVA) registration plate number: 2AW1295; and
3) 2002 Black Ford Taurus, with VIN: 1FAFP55222A20434, bearing Maryland MVA registration plate number: 3AK5680.

Owned, Used, or Operated by RAMOS-AGUSTIN:

4) The residence located at 647 High Street, in Cambridge, Maryland 21613;
5) 2000 Gray Toyota Corolla, with VIN: 1NXBR12E3YZ403371, bearing Maryland MVA: 1AN6236; and
6) 1998 Black Lincoln Continental, with VIN: 1LNFM97V6WY664345; bearing Maryland MVA registration plate number: 1AZ4654.

As set forth below, there is probable cause to believe that CRUZ-CRUZ, a Mexican national and citizen residing in the basement apartment of 10505 Truxton Road in Adelphi, Maryland 20783 and RAMOS-AGUSTIN, a Guatemalan national and citizen residing at 647 High Street in Cambridge, Maryland 21613 have violated Title 18 USC §§ 1028, 1028A, and 1546, and Title 42 USC § 408. Further, there is probable cause to believe that the fruits and evidence related to violations of Title 18 USC §§ 1028, 1028A and 1546, and Title 42 USC § 408 will be found in the residence and vehicles of CRUZ-CRUZ: 10505 Truxton Road, Basement Apartment, in Adelphi, Maryland 20783; a 2000 Gold Chevy Tahoe with VIN

1GNEK13T5YJ103097, bearing Maryland MVA registration plate number 2AW1295; and a 2002 Black Ford Taurus with VIN 1FAFP55222A20434, bearing Maryland MVA registration plate number 3AK5680, and in the residence and vehicles of RAMOS-AGUSTIN: 647 High Street in Cambridge, Maryland 21613; a 2000 Gray Toyota Corolla with VIN 1NXBR12E3YZ403371, bearing Maryland MVA registration plate number 1AN6236; and a 1998 Black Lincoln Continental with VIN 1LNFM97V6WY664345, bearing Maryland MVA registration plate number 1AZ4654.

REVELANT STATUTES

Title 18, Section 1028(a)(3) renders it unlawful for a person to knowingly possess an identification document (other than one issued lawfully for the use of the possessor) or a false identification document, with the intent such document be used to defraud the United States. Your affiant is also aware that illegal aliens often seek to obtain fraudulent identities in order to illegally enter and/or remain in the United States in violation of the law.

Title 18, Section 1028A, renders it unlawful for a person to knowingly possess, use or transfer the means of identification of another individual in relation to a variety of underlying offenses, including document fraud, fraud and misuse of immigration documents and social security number fraud.

Title 18 U.S.C. §1546 renders it unlawful for a person to knowingly forge, counterfeit, alter or falsely make any immigrant or nonimmigrant visa, permit, border crossing card, alien registration receipt card or other documents prescribed by statue or regulation for entry into or as evidence of authorized stay or employment in the United States.

Title 42 U.S.C. § 408(a)(7)(C) renders it unlawful to alter a social security number card or to buy or sell a counterfeit social security number card.

BACKGROUND

1. On or about October 2011, HSI SAC Baltimore learned of an individual known as "TONY," later identified as CRUZ-CRUZ, who worked for a criminal organization involved in the manufacture and distribution of fraudulent documents primarily in the Hyattsville and Langley Park, Maryland area. The Hyattsville, Langley Park area is commonly known as an area where foreign nationals can purchase fraudulent documents in order to conceal their identity and/or unlawful status in the United States. This investigation has shown that CRUZ-CRUZ and others, known and unknown, have distributed the following fraudulent documents:

a) fraudulent Permanent Resident Cards (Form I-551);

b) fraudulent Employment Authorization Cards (Form I-766);

c) fraudulent Social Security Number Cards (Form SSA-3000);

d) fraudulent U.S. driver's licenses, including, but not limited to the State of Maryland; and

e) fraudulent foreign driver's licenses, including, but not limited to Mexican driver's licenses.

2. According to a HSI Confidential Source, hereinafter referred to as "CS1," there are multiple individuals, including CRUZ-CRUZ, involved in the production fraudulent of identification documents.

3. According to CS1, CRUZ-CRUZ utilizes the following telephone number: (443) 676-5678. Law enforcement officers have not yet identified a connection between CRUZ-CRUZ and the individual this telephone number is registered to, but there is a connection between CRUZ-CRUZ and the prior user of this number. This number was previously used by another individual known as "Puma," who was involved in a document trafficking organization called the

"Broadway Organization." The Broadway Organization operated on the 200 block of South Broadway in Baltimore, Maryland. The Broadway Organization was the subject of a federal indictment in 2011 and ten of its members have been convicted over the past year. When arrests were made in the Broadway case, Puma left the United States and returned to Mexico. Based upon your affiant's experience investigating document fraud cases, the telephone number of a document vender, such as Puma's, has value because it has been circulated in the community as a contact number for persons looking for fraudulent documents. Generally, such telephone numbers are sold to other document venders when one is arrested. It is believed this is how CRUZ-CRUZ obtained the number.

4. CRUZ-CRUZ's organization typically works in the following manner. Individuals known as "vendors" obtain orders from customers who wish to purchase one or more fraudulent identity document for a negotiated price. The customer will provide the vendor with name and other identifying information, such as birth date, county of citizenship, address, or social security number that should be included on the fraudulent identity document. Many of the documents require a photograph of the customer. This information, including the photograph, must be sent to CRUZ-CRUZ or any of his associates so that it can be used to create the fraudulent identity document. The customer will provide either the information directly to the vendor or will send the identifying information and/or photograph directly to a member of the organization via text message and picture message. Members of the organization will call one another to discuss and confirm receipt of the identifying information and photographs and to arrange the times and locations for distributing the completed fraudulent identity document to the customer. Based upon the investigation to date, your affiant believes that CRUZ-CRUZ manufactures and sells the counterfeit documents, takes orders for counterfeit documents directly

from customers, as well as receiving orders for counterfeit documents from other members of the organization, and obtains counterfeit document making supplies. Once the fraudulent identity documents are ready, usually within several hours, the vendor can obtain them from CRUZ-CRUZ and then meet the customer to deliver the fraudulent identity documents in exchange for money.

5. RAMOS-AGUSTIN is a document vendor based in Cambridge, Maryland, who obtains counterfeit documents from CRUZ-CRUZ and sells those documents on the Eastern Shore of Maryland.

INVESTIGATION OF CRUZ-CRUZ

6. On October 17, 2011, a Confidential Source, hereinafter referred to as "CS2," made a consensually recorded telephone call to a telephone number believed to be associated with this organization, but not the number used by CRUZ-CRUZ. CS2 initiated a purchase of two sets of fraudulent identity documents. The sets consisted of a Permanent Resident Card and a Social Security Number Card and cost $120.00. CS2 informed the document vendor that he/she would contact him when the photos and information needed for the documents were ready.

7. On October 24, 2011, CS2 made a consensually recorded telephone call to CRUZ-CRUZ, who agreed to supply the fraudulent documents previously negotiated on October 17, 2011. In addition, CRUZ-CRUZ informed CS2 to send the photographs and information needed to fabricate the documents to him. CS2 followed the directions and sent the required photographs and information via text messages to CRUZ-CRUZ.

8. On October 25, 2011, CS2 arrived at the meeting location in the District of Maryland and encountered CRUZ-CRUZ. During the meeting, CRUZ-CRUZ was driving a

2002 Black Ford Taurus bearing Maryland MVA registration plate number 3AK5680 and VIN 1FAFP55222A20434, hereinafter referred to as "BLACK TAURUS." CRUZ-CRUZ gave CS2 the counterfeit identification documents in exchange for $240.00. During the meeting, CRUZ-CRUZ gave CS2 several business cards which advertised fictitious services. These cards contained multiple telephone numbers, including the initial phone number CS2 had called on October 17, 2011, and CRUZ-CRUZ's number. The cards were provided to CS2 to distribute to individuals seeking to purchase counterfeit identity documents. After the transaction CRUZ-CRUZ was observed by CS2 entering the La Union Mall, located at 1401 University Boulevard E, in Hyattsville, Maryland 20783, and then departing the area in the BLACK TAURUS. Later that evening CS2 made a consensually recorded telephone call to CRUZ-CRUZ and stated the cards looked great and asked if CRUZ-CRUZ could provide driver's licenses for CS2's clients. CRUZ-CRUZ replied that he could provide driver's licenses from anywhere (state/country) CS2 wanted.

9. On November 22, 2011, CS2 made a consensually recorded telephone call to CRUZ-CRUZ at the same telephone number CS2 called on October 17, 2011, and initiated the purchase of four sets of fraudulent identity documents consisting of three Permanent Resident Cards and four Social Security Number Cards and one State of Maryland driver's license for $480.00. During the conversations CS2 was asked to send the photographs and information needed to fabricate the documents to CRUZ-CRUZ's telephone number. CS2 followed the directions and sent the required photographs and information via text messages to that number.

10. On November 23, 2011, CS2 met with CRUZ-CRUZ in the District of Maryland. During this meeting, CRUZ-CRUZ was driving the BLACK TAURUS. Upon arrival, CRUZ-CRUZ gave CS2 eight fabricated identification documents in exchange for $480.00. After the

transaction CRUZ-CRUZ was observed driving the BLACK TAURUS from one parking spot to another and then entering the La Union Mall. A few minutes later he exited the mall, entered the BLACK TAURUS and drove Eastbound on various side streets until reaching Riggs Road were surveillance was terminated.

11. On August 27, 2012, a HSI Confidential Source, hereinafter referred to as "CS3," made a consensually recorded telephone call to CRUZ-CRUZ. During this call, CS3 told CRUZ-CRUZ that he/she was following up on a conversation they previously had. CRUZ-CRUZ replied that a lot of people call him. CS3 told CRUZ-CRUZ that he/she was interested in obtaining immigration documents. CRUZ-CRUZ offered CS3 documents of varying quality and ultimately agreed to sell CS3 a Permanent Resident Card and a Social Security NumberCard for $200.00. Later that day, CS3 received a text message from CRUZ-CRUZ asking if CS3 was still interested in going through with the purchase. Via text messages on August 27th and 28th, CS3 confirmed the purchase of fraudulent documents and set up a meeting for August 29, 2012 to purchase the documents for $200.00 in cash, and sent CRUZ-CRUZ a text message containing his/her photo, name, date of birth and a country of birth to be placed on the fraudulent cards.

12. On August 29, 2012, CS3 met CRUZ-CRUZ at a location previously specified by CRUZ-CRUZ, the Dunkin' Donuts parking lot, located at 2057 University Blvd E, Hyattsville, Maryland. CRUZ-CRUZ arrived late, driving the BLACK TAURUS, and when CS3 asked CRUZ-CRUZ why he was late, CRUZ-CRUZ stated the original documents that were created contained errors and the documents needed to be re-made. CRUZ-CRUZ provided CS3 with an envelope containing a fraudulent Permanent Resident Card and a fraudulent Social Security Number Card containing the information that CS3 sent to CRUZ-CRUZ via text message. CS3 provided CRUZ-CRUZ with $200.00 in cash.

13. On October 24, 2012, a federal grand jury in the District of Maryland issued an indictment for CRUZ-CRUZ for violations of Title 18, U.S.C. § 1028, Fraud and Related Activity in connection with Identification Documents; Title 18, U.S.C. § 1546, Misuse of Immigration Documents; Title 42, U.S.C. § 408, Social Security Number Fraud and Title 18, U.S.C. § 2, Aiding and Abetting.

14. On November 6, 2012, an HSI Confidential Source, hereinafter referred to as "CS4", made a consensually monitored telephone call to CRUZ-CRUZ. CS4 initiated the purchase of a set of fraudulent identity documents. The sets consisted of a Permanent Resident Card and a Social Security Number Card and cost $110.00 or $140.00. CS4 sent CRUZ-CRUZ a text message containing his/her photo, name, date of birth and a country of birth to be placed on the fraudulent cards.

15. On November 8, 2012, CRUZ-CRUZ contacted CS4 by text message and phone call, which was not monitored and recorded, and arranged to meet at the Galaxy Bar, in Hyattsville, Maryland. (The Galaxy Bar and Grill is located in the rear of the same shopping center of the Dunkin' Donuts parking lot, located at 2057 University Blvd E, Hyattsville, Maryland.) This time CRUZ-CRUZ arrived at the meet location in a 2000 Gold Chevy Tahoe bearing Maryland MVA registration plate number 2AW1295 and VIN 1GNEK13T5YJ103097, hereinafter referred to as "GOLD TAHOE." Upon CRUZ-CRUZ's arrival, CS4 entered the GOLD TAHOE. CRUZ-CRUZ provided CS4 a fraudulent Permanent Resident Card and Social Security Number Card, containing the information CS4 had sent via text message on November 6, 2012, in exchange for $110.00. A few minutes later, CS4 exited entered his/her vehicle and departed the area. CRUZ-CRUZ exited the GOLD TAHOE and walked over to an unknown

vehicle parked nearby. CRUZ-CRUZ entered the unknown vehicle and appeared to exchange something with an unknown individual inside the vehicle. CRUZ-CRUZ then returned to the GOLD TAHOE. A few minutes later, another unknown individual in a second unknown vehicle parked next to the GOLD TAHOE. The unknown individual exited his vehicle and entered the GOLD TAHOE, appeared to be exchanging documents and then returned to his vehicle and departed.

16. Agents conducted mobile surveillance of CRUZ-CRUZ after he departed the parking lot. He made several stops before pulling over in front of 10505 Truxton Road, in Adelphi, Maryland, hereinafter "TRUXTON Residence." CRUZ-CRUZ opened the hood of the GOLD TAHOE and appeared to be inspecting the engine. Mobile surveillance was terminated at this time as CRUZ-CRUZ appeared to be conducting counter surveillance. At approximately 04:00 hours the next morning an agent conducted a drive-by of the TRUXTON Residence and observed the GOLD TAHOE parked in front, right behind the BLACK TAURUS, used by CRUZ-CRUZ.

17. On November 19, 2012, CS4 made a consensually monitored telephone call to CRUZ-CRUZ. CS4 initiated the purchase of a set of fraudulent identity documents. The set consisted of a Permanent Resident Card and a Social Security Number Card and cost $110.00. Following the telephone call CS4 sent CRUZ-CRUZ a text message with the picture and biographical information to be placed on the fraudulent cards and to confirm the location to meet for the exchange, the parking lot of Dunkin' Donuts, located at 2057 University Blvd E, in Hyattsville, Maryland. Approximately 2 hours after the call was made, CRUZ-CRUZ arrived at the meet location in the GOLD TAHOE. CRUZ-CRUZ called CS4 to find out his/her location. CS4 described their vehicle and their location in the parking lot. CRUZ-CRUZ parked next to

CS4 and CS4 entered the GOLD TAHOE. CRUZ-CRUZ sold CS4 a fraudulent Permanent Resident Card and a Social Security Number Card, containing the information CS4 had sent via text message earlier that day. CRUZ-CRUZ also gave CS4 several business cards to pass to others who were interested in obtaining cards. CS4 exited the GOLD TAHOE and entered his/her vehicle and drove away. On November 19, 2012, agents maintained continuous surveillance of CRUZ-CRUZ's residence, the TRUXTON Residence, prior to the initial call being made and maintained surveillance of CRUZ-CRUZ from the TRUXTON Residence to the meet location for the transfer of documents to CS4. Agents observed CRUZ-CRUZ exiting the TRUXTON Residence from the basement entrance, entering the GOLD TAHOE, and driving away. At no time after leaving the TRUXTON Residence did CRUZ-CRUZ stop or meet with anyone during his drive to the meet location at 2057 University Blvd E, in Hyattsville, Maryland.

18. On January 22, 2013, a HSI Confidential Source, hereinafter referred to as "CS5," made a consensually monitored call to a telephone number belonging to a document vendor, Ricardo LOPEZ-CRUZ (LOPEZ-CRUZ is the maternal cousin of CRUZ-CRUZ who previously ran a document mill in the Baltimore Washington area who went into hiding after the Broadway Organization arrests in 2011.) CS5 initiated the purchase a set of fraudulent identity documents with the individual that answered the telephone call. The set consisted of a Permanent Resident Card and a Social Security Number Card and cost $130.00. Following the telephone call CS5 sent LOPEZ-CRUZ a text message containing his/her photo, name, and date of birth to be placed on the fraudulent cards. CS5 called LOPEZ-CRUZ to confirm he received the text message and to confirm the time and location for the meet for the exchange, the parking lot of Coco Cabana Bar and Grill, located at 2031 E University Blvd E, Hyattsville, Maryland. (The Coco Cabana

Bar and Grill is located in the rear of the same shopping center of the Dunkin' Donuts located at 2057 University Blvd E, Hyattsville, Maryland.)

19. On January 23, 2013, CS5 arrived at the meeting location in the District of Maryland, and made an unmonitored call to LOPEZ-CRUZ to inform him he arrived. Approximately 25 minutes later CRUZ-CRUZ arrived at the meet location driving the GOLD TAHOE. CRUZ-CRUZ parked next to CS5's vehicle and told him/her to get in since it was cold outside. CS5 entered the GOLD TAHOE and provided $130.00 to CRUZ-CRUZ in exchange for a fraudulent Permanent Resident Card and Social Security Number Card containing the information CS5 had sent via text message on January 22, 2013. After the exchange of documents CRUZ-CRUZ stated if CS5 was to order 3 or more sets of documents it would cost $90.00 a set. CS5 exited the GOLD TAHOE and returned to his vehicle while CRUZ-CRUZ exited the parking lot.

20. On January 23, 2013, HSI Special Agents were conducting simultaneous surveillance of the TRUXTON Residence and observed CRUZ-CRUZ depart from the basement of the TRUXTON Residence, enter the GOLD TAHOE and drive off. Approximately 20 minutes later CRUZ-CRUZ arrived at the meet location. An HSI Special Agent drove the three different main routes from the TRUXTON Residence to the meet location, the Coco Cabana Grill, located at 2031 E University Blvd E, Hyattsville, Maryland. The agent made the drive in an average of 15 to 20 minutes.

INVESTIGATION OF RAMOS-AGUSTIN

21. On or about September 2012, HSI Resident Agent in Charge office in Ocean City, Maryland, (RAC-OC) learned of an individual identified as RAMOS-AGUSTIN, living in

Cambridge, Maryland, involved in the distribution of fraudulent documents on the Eastern Shore, Maryland.

22. On or about October 10, 2012, a RAC-OC Confidential Source, hereinafter referred to as "CS6," made a consensually monitored call to RAMOS-AGUSTIN to inquire about purchasing fraudulent identity documents. RAMOS-AGUSTIN stated he could provide a set of documents, a Permanent Resident Card and a Social Security Number Card, for $125.00. CS6 stated he/she would contact RAMOS-AGUSTIN the following week to arrange a time to meet to purchase the fraudulent documents.

23. On or about October 17, 2012, RAMOS-AGUSTIN met CS6 in the parking lot of the Wal-Mart, in Easton, Maryland, driving a 2000 Gray Toyota Corolla, with VIN 1NXBR12E3YZ403371, bearing Maryland MVA registration plate number 1AN6236, hereinafter referred to as "GRAY TOYOTA." During this meeting RAMOS-AGUSTIN took a photo of CS6, using his mobile phone, to use on the Permanent Resident Card and stated he will send the photo to the Mexican guy he works for who makes the documents. CS6 advanced RAMOS-AGUSTIN $80.00 as a down payment for the documents. Approximately 3 hours later, on October 17, 2012, RAMOS-AGUSTIN met CS6, in the parking lot of the Kmart on Kent Island, Maryland, again driving the GRAY TOYOTA. RAMOS-AGUSTIN provided CS6 with the fraudulent Permanent Resident Card and Social Security Number Card, containing the information and photo CS6 had given RAMOS-AGUSTIN earlier that day. CS6 paid RAMOS-AGUSTIN balance due, $45.00, for the documents. After the document purchase, CS6 inquired about obtaining real identity documents that would come back to a real person if the social security number was checked by an employer. RAMOS-AGUSTIN stated he could possibly obtain real identity documents from Texas and it would cost between $500.00 and $800.00

dollars. RAMOS-AGUSTIN was followed back to his residence located at 647 High Street, in Cambridge, Maryland 21613, hereinafter referred to as the "HIGH STREET Residence."

24. On or about November 28, 2012, CS6 made a consensually monitored call to RAMOS-AGUSTIN. CS6 inquired about the purchase of fraudulent documents and a real identity document. RAMOS-AGUSTIN stated he would call his supplier to get a price for the Social Security Number Cards and call CS6 back. RAMOS-AGUSTIN also stated that the real identity document he had is for a female and it would cost $350. Approximately 5 minutes later RAMOS-AGUSTIN called CS6 back and informed him/her it would cost $40.00 for each Social Security Number Card and the real identity belonged to a Puerto Rican female.

25. On or about December 3, 2012, CS6 made a consensually monitored call to RAMOS-AGUSTIN to arrange to meet the next day to purchase the fraudulent Social Security Number Cards. RAMOS-AGUSTIN and CS6 agreed to meet at the Kmart on Kent Island, Maryland the next day.

26. On or about December 4, 2012, CS6 made a consensually monitored call to RAMOS-AGUSTIN to initiate the purchase of fraudulent documents, five fraudulent Social Security Number Cards. RAMOS-AGUSTIN arrived at the meet location driving the GRAY TOYOTA. CS6 provided RAMOS-AGUSTIN the names for the Social Security Number Cards and $100 down payment for the cards. RAMOS-AGUSTIN said he would return in approximately an hour and a half. Mobile surveillance followed RAMOS-AGUSTIN to the Giant Food store parking lot located at 3521 East-West Highway, in Hyattsville, Maryland. RAMOS-AGUSTIN met with CRUZ-CRUZ, who was driving the GOLD TAHOE. Special Agents observed what appeared to be identity documents passed from CRUZ-CRUZ to RAMOS-AGUSTIN, and soon after both vehicles departed the area. Later that evening at the

original meet location on Kent Island, RAMOS-AGUSTIN arrived in the GRAY TOYTOTA and gave CS6 a small envelope containing five fraudulent Social Security Number Cards containing the information CS6 had given RAMOS-AGUSTIN earlier that day. CS6 then paid RAMOS-AGUSTIN the remaining $100.00 balance, for a total of $200.00 paid. CS6 stated he/she was interested in obtaining the Puerto Rican identity documents previously discussed with RAMOS-AGUSTIN.

27. On February 18, 2013, CS6 initiated the purchase of genuine Puerto Rican identity documents, a counterfeit Maryland ID Card, and two counterfeit Social Security Number Cards from RAMOS-AGUSTIN through text messages. CS6 inquired as to the exact price of the documents. RAMOS-AGUSTIN stated the Puerto Rican Birth Certificate would cost $350.00, the counterfeit Maryland ID would cost $100.00 and the two counterfeit Social Security Number Cards would cost $80.00, for a total of $530.00. RAMOS-AGUSTIN stated he would need the money for the genuine Puerto Rican Birth Certificate and half the money for the counterfeit Maryland ID and two counterfeit Social Security Number Cards up front. CS6 and RAMOS-AGUSTIN agreed to meet at the Kmart on Kent Island, Maryland, the next day to conduct the transaction.

28. On February 19, 2013, CS6 sent RAMOS-AGUSTIN the photo to be used on the counterfeit Maryland ID and the names to be used on the counterfeit Social Security Number Cards by text message. CS6 and RAMOS-AGUSTIN met at the parking lot of the Kmart on Kent Island. RAMOS-AGUSTIN arrived in a 1998 Lincoln Continental with VIN 1LNFM97V6WY664345 and bearing Maryland MVA registration plate number 1AZ4654, hereinafter referred to as "BLACK LINCOLN," and had an unknown Hispanic male in the front passenger seat. RAMOS-AGUSTIN and CS6 spoke for several minutes before RAMOS-

AGUSTIN gave CS6 the genuine Puerto Rican Birth Certificate and genuine Social Security Number Card (ending in 4343) with the initials of "BAV," a real person born in Puerto Rico. RAMOS-AGUSTIN stated he would return with the other documents in a few hours. Mobile surveillance followed the BLACK LINCOLN to the La Union Mall, at 1401 University Boulevard E, in Hyattsville, Maryland.

29. On February 19, 2013, HSI Special Agents were conducting simultaneous surveillance of the TRUXTON Residence and observed CRUZ-CRUZ departed from the basement entrance the TRUXTON Residence with an unknown Hispanic male and enter the BLACK TAURUS and drive off. Approximately 15 minutes after departing the TRUXTON Residence, the BLACK TAURUS, driven by CRUZ-CRUZ arrived at the Dunkin Donuts located 2057 University Blvd E, Hyattsville, Maryland and parked next to BLACK LINCOLN, driven by RAMOS-AGUSTIN. Both vehicles departed the area a few minutes later. RAMOS-AGUSTIN then proceeded directly to the Kmart on Kent Island and upon arriving met with CS6 and provided CS6 with a small white envelope containing a counterfeit Maryland ID Card in the name of "BAV" and two counterfeit Social Number Security Cards containing the information CS6 had sent via text message earlier that day. CS6 noticed several other small white envelopes similar to the one RAMOS-AGUSTIN gave CS6 inside the BLACK LINCOLN. Several minutes later, RAMOS-AGUSTIN departed and surveillance followed him east on Route 50. RAMOS-AGUSTIN stopped briefly at a residence located at 22826 Marsh Creek Road, Preston, MD and went up to the front door of the residence and then back to the BLACK LINCOLN. RAMOS-AGUSTIN then dropped his passenger off at Academy and Main Street in Cambridge, Maryland before arriving at the HIGH STREET Residence, where he parked the car and went inside.

ADDITIONAL INVESTIGATION

30. Your affiant conducted surveillance on January 18, 2013 from 10:00 a.m. to 12:00 noon and both the GOLD TAHOE and the BLACK TAURUS were parked in front of the TRUXTON Residence with no movement. Your affiant also conducted surveillance on February 5, 2013 from approximately 5:00 p.m. to 7:00 p.m. and observed only the BLACK TAURUS parked near the home and no movement. Your affiant also conducted surveillance at the TRUXTON Residence on March 14, 2013. At approximately10:00 a.m. when the surveillance began, the GOLD TAHOE was parked in front of the TRUXTON Residence and the BLACK TAURUS was parked directly across the street. At approximately 12:50 p.m., CRUZ-CRUZ exited the residence from the basement entrance and drove away in the GOLD TAHOE.

31. On March 13, 2013, at approximately 10:30 a.m. an agent conducted surveillance on the HIGH STREET Residence. The GREY TOYOTA was parked in front of the residence.

32. During the investigation, agents checked the registration of each vehicle which CRUZ-CRUZ and RAMOS-AGUSTIN were observed driving. A review of Maryland MVA records revealed CRUZ-CRUZ has used the identity of a real person born in Puerto Rico, "FDP," to register the GOLD TAHOE. The BLACK TAURUS was registered in the name of a female believed to be CRUZ-CRUZ's girlfriend.

33. A review of Maryland MVA records for "FDP" revealed that CRUZ-CRUZ had obtained a genuine Maryland driver's license in the name of "FDP" and that he had provided that identification to law enforcement when he was stopped for a traffic violation. Agents obtained records from Puerto Rico, including fingerprints and photographs of "FDP," which establish conclusively that CRUZ-CRUZ is not "FDP" but is using the means of identification (name, date of birth, and social security number) of "FDP."

34. Maryland MVA records show both the GRAY TOYOTA and the BLACK LINCOLN are registered to RAMOS-AGUSTIN at his residence at the HIGH STREET Residence.

35. On March 20, 2013, a federal grand jury in the District of Maryland issued a Superseding Indictment charging both CRUZ-CRUZ and RAMOS-AGUSTIN with violations of Title 18, U.S.C. § 1028, Fraud and Related Activity in connection with Identification Documents; Title 18, U.S.C. §1028A, Aggravated Identity Theft; Title 18, U.S.C. § 1546, Misuse of Immigration Documents; Title 42, U.S.C. § 408, Social Security Number Fraud and Title 18, U.S.C. § 2, Aiding and Abetting.

TRAINING AND EXPERIENCE ON DOCUMENT VENDORS

36. Based on knowledge and experience, the following is commonly known to occur as it relates to persons involved in the manufacture and trafficking of fraudulent identity and employment eligibility documents in high volume:

a) Document vendors maintain books, records, receipts, notes, ledgers, money orders, IOU's, money owed lists, and other items relating to the selling of fraudulent identity and employment eligibility documents and these are often found at the location where they conduct their illegal activity and their place of residence. Often, such documentary evidence is written or recorded in a code to maintain the secret nature of such illegal enterprises.

b) That the aforementioned books, records, receipts, notes, ledgers, money orders, IOU's, buyer and seller lists, and other items are commonly maintained where document vendors have ready access to them (e.g. homes, businesses, storage lockers, or automobiles.) These records are commonly maintained for an extended period of

time, much as a legitimate business might maintain records of purchases, distributions, and accounts payable/receivable, especially true when illegal document fraud activities are carried out over an extended period of time.

c) It is common for document vendors to conceal the proceeds of such sales and records of these transactions, sources, and/or customers, in secure locations within homes, businesses, storage facilities, safe deposit boxes, and automobiles.

d) That such individuals and organizations involved in such large-scale document trafficking commonly conceal in their homes, businesses, storage lockers, safety deposit boxes, or automobiles, large amounts of currency, financial instruments, precious metals, jewelry, and other things of value gained from their criminal enterprise.

e) That when vendors amass large sums of document vending related proceeds, they often attempt to legitimize their profits so that they may spend their profits without incurring scrutiny of law enforcement officials.

f) To accomplish these goals, document vendors often send money out of the country using wire transfers as well as domestic and foreign banks and their attendant services.

g) That document traffickers involved in high sales very often maintain residences and assets (e.g. vehicles, rental houses, real estate holdings, etc.) under fictitious names or under the names of the other persons such as relatives, spouses or girlfriends and/or associates to avoid detection by law enforcement officials. Despite the listing under fictitious or other holdings, document vendors will continue to exercise dominion and control over these assets.

h) That document traffickers commonly maintain address and/or telephone numbers in books or papers which reflect names, addresses, and/or telephone numbers of their associates in criminal organizations and records of their transactions. Often these names, addresses, or numbers may be in code.

i) That document traffickers frequently take, or cause to be taken, photographs of their associates, their property, and their products. Document traffickers maintain their photographs in their homes, businesses, storage lockers, safety deposit boxes, and automobiles. These photographs will often reflect the document traffickers and members of their organization together, as well as aspects of their lifestyle that involve the document fraud.

j) That document vendors also commonly use electronic text devices and mobile telephones to communicate with their customers. Such devices have memory storage capabilities that store return telephone numbers or frequently called telephone numbers used by the subscriber.

k) That document traffickers involved in the manufacture of a high volume of fraudulent documents frequently use, own or possess firearms. These individuals commonly and ordinarily keep those firearms, in their residence, in their vehicles, or in vehicles over which they have dominion and control.

l) That document traffickers who use, own or possess firearms also commonly and ordinarily possess other items indicating the possession of firearms, including, but not limited to, ammunition, photographs of the firearms or of themselves in possession of firearms, holsters, firearm cleaning equipment, spare parts for firearms, and receipts

and repair bills for firearms. These items are commonly and ordinarily kept on their person, in their residences, or in vehicles over which they have dominion and control.

m) That these individuals commonly and ordinarily keep documents or indicia that are evidence of the occupancy or ownership of their premises and their vehicles. These documents and indicia are ordinarily to be found on their person or in their premises or in the vehicles they own or use. Such documents or indicia include, but are not limited to, utility bills, rent receipts, payment receipts, personal mail or other correspondence addressed at the residence, and vehicle registration information, ownership warranties, or receipt for parts.

37. Based on your Affiant's experience, document counterfeiters frequently produce identity documents within their places of residence, facilitating the prompt manufacturing of fraudulent documents. It is your affiant's experience that devices utilized in the creation of fraudulent identity documents are commonly found to be located in the place of principal residence, including but not limited to computers, ordinary office printers, special plastic card printers, laminating machines, cutting machines, and other general office and specialized equipment to manufacture counterfeit identification documents. Moreover, individuals engaged in the manufacture of counterfeit identity documents also use various specialty and off-the-shelf computer programs, as well as document templates, to manufacture counterfeit identification documents. It is your affiant's experience that back up copies of the software and templates used to fabricate fraudulent documents are kept within their places of residence for safekeeping.

38. Your affiant knows that individuals engaged in the manufacture of counterfeit identity documents maintain supplies needed for the manufacture of such documents, including special paper, blank plastic cards, special ribbons for card printers, materials for lamination of

cards, metallic or film materials used to create the illusion of holograms, actual holographic stickers or materials, and other items used in the manufacture of counterfeit identity documents.

39. Your affiant knows that the manufacture of counterfeit identity documents generates actual counterfeit identity documents as well as by-products such as flawed or misprinted identity documents, either whole or shredded, as well as scraps of paper, backing off of holographic stickers, used ribbons, and other materials which are often found in document mills.

40. Your affiant knows that it is common for document manufacturers, document venders, and their co-conspirators to also use computers to create advertisements used to promote the illegal activity, fraudulent identifications, licenses and employee identifications, as well as to store information concerning money laundering on a computer in order to conceal it from law enforcement authorities. Your affiant knows that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentality, fruits, or evidence of a crime, and/or (2) the objects may have been used to collect and store information about crimes in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentality, fruits, or evidence of a crime; or (2) storage devices for information about a crime.

41. Through training and experience, your affiant knows that fraudulent document manufacturers and venders generally prefer to store images of fraudulent identification documents in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for fraudulent identification documents. A small

portable digital memory device can contain hundreds or thousands of images of fraudulent identification documents, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of fraudulent identification documents, and the digital memory devices that contain the files, can be mislabeled or hidden to evade detection. Your affiant knows that the creators of fraudulent documents often use items such as computer hardware, software, related documentation, digital cameras, and scanners to create fraudulent documents.

SEIZURE AND SEARCH OF DIGITAL DEVICES

42. As used below, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes used to store digital data (excluding analog tapes such as VHS), and memory chips; and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of the premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data, that, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it,

and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of

particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment.

CONCLUSION

43. Based on the foregoing, your affiant respectfully submits that there is probable cause to believe that the following items, which constitute evidence, fruits and instrumentalities of violations of 18 USC §§ 1028, 1028A, 1546, and Title 42 USC § 408 will be found in the following locations and in the following vehicles:

a. 10505 Truxton Road, Basement Apartment, in Adelphi, Maryland 20783;

b. 2000 Gold Chevy Tahoe with VIN 1GNEK13T5YJ103097, bearing Maryland MVA registration plate number 2AW1295;

c. 2002 Black Ford Taurus with VIN 1FAFP55222A20434, bearing Maryland MVA registration plate number 3AK5680;

d. 647 High Street, in Cambridge, Maryland 21613;

e. 2000 Gray Toyota Corolla with VIN 1NXBR12E3YZ403371, bearing Maryland MVA registration plate number 1AN6236; and

13-0579TJS – 13-0584TJS

f. 1998 Lincoln Continental with VIN 1LNFM97V6WY664345, bearing Maryland MVA registration plate number 1AZ4654);

all described more fully in Attachment A.

Lyndon George, Special Agent
U.S. Immigration and Customs Enforcement
Homeland Security Investigations

Sworn to before me this
25th day of March, 2013

Timothy J. Sullivan
United States Magistrate Judge
District of Maryland

13-0579TJS – 13-0584TJS

Attachment A

Describe in detail the locations to be searched and attach at least one photograph of each.

The Premises, known as 10505 Truxton Road, Adelphi, Maryland 20783, is described as a two story split level house with white siding over tan brick, with the numbers "10505," in black letters to the left above the entrance door. The entrance to target apartment (the Basement Apartment) is on the lower level right side of residence with gray entrance door with outdoor light to the left. There is a stone walkway to the door.

13-0579TJS -13-0584TJS

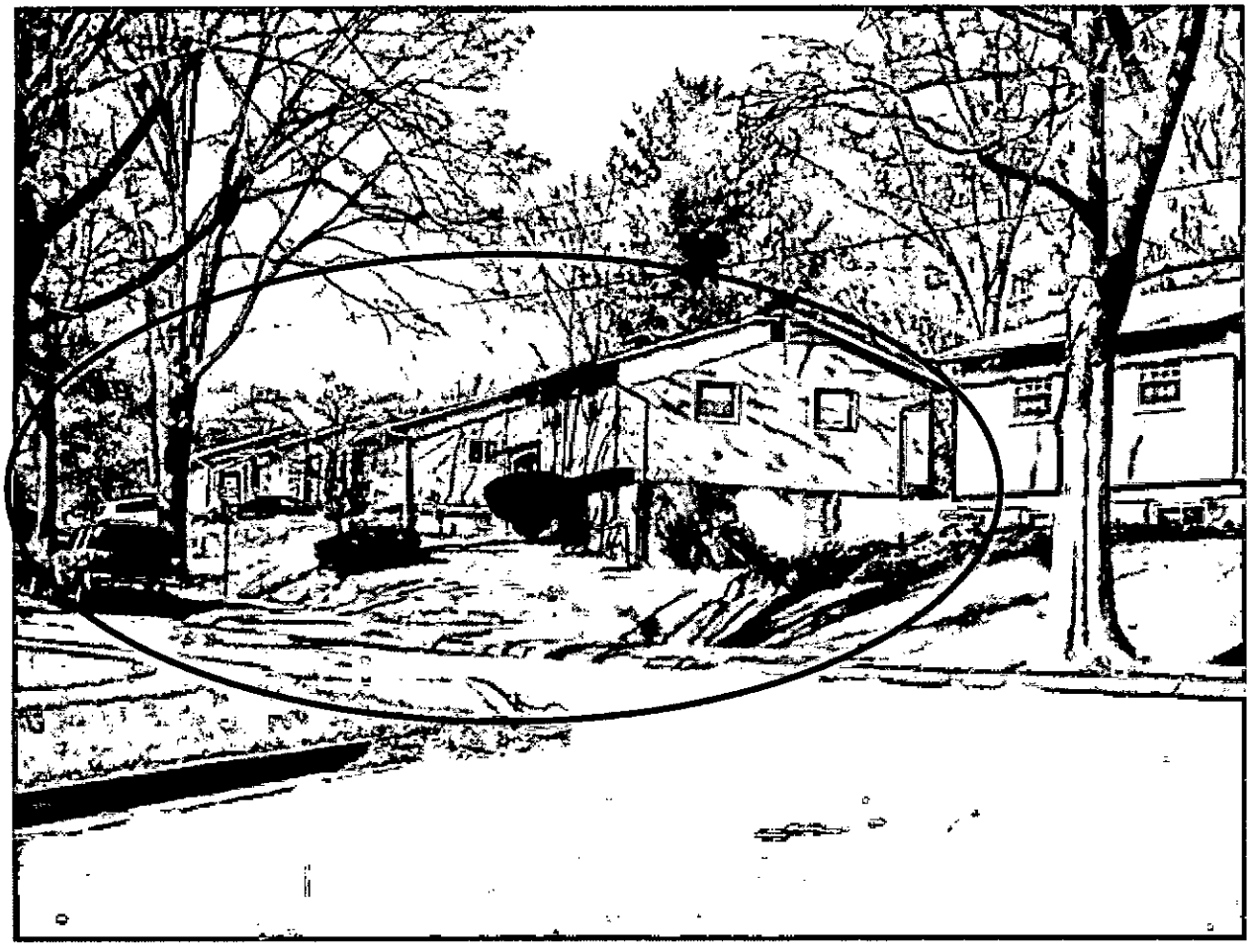
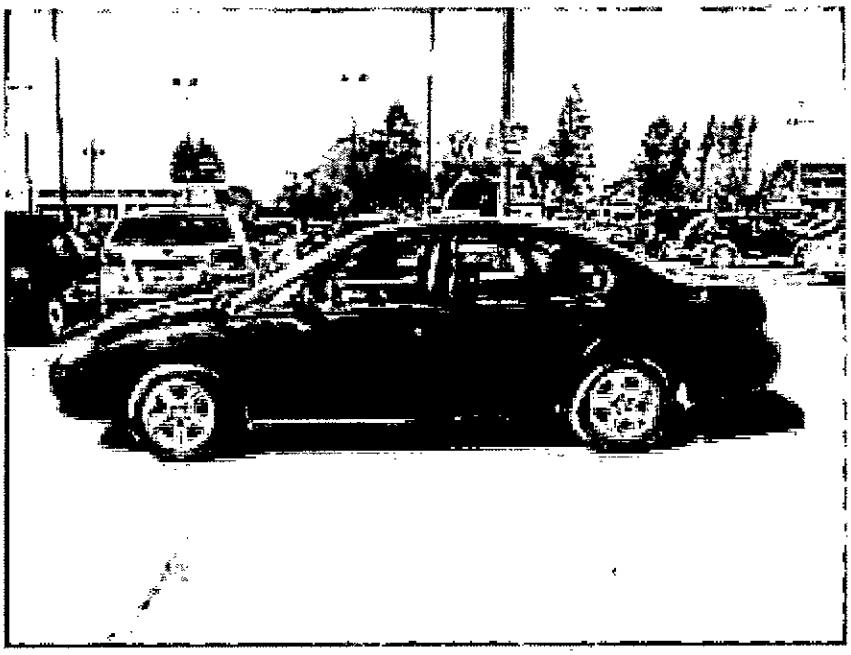


Photo of target after exiting the Basment Apartment, gray door to the right of target at

10505 Truxton Road, Adelphi, MD 20783.

13-0579TJS - 13-0584TJS



2002 Black Ford Taurus, with VIN: 1FAFP55222A20434, bearing

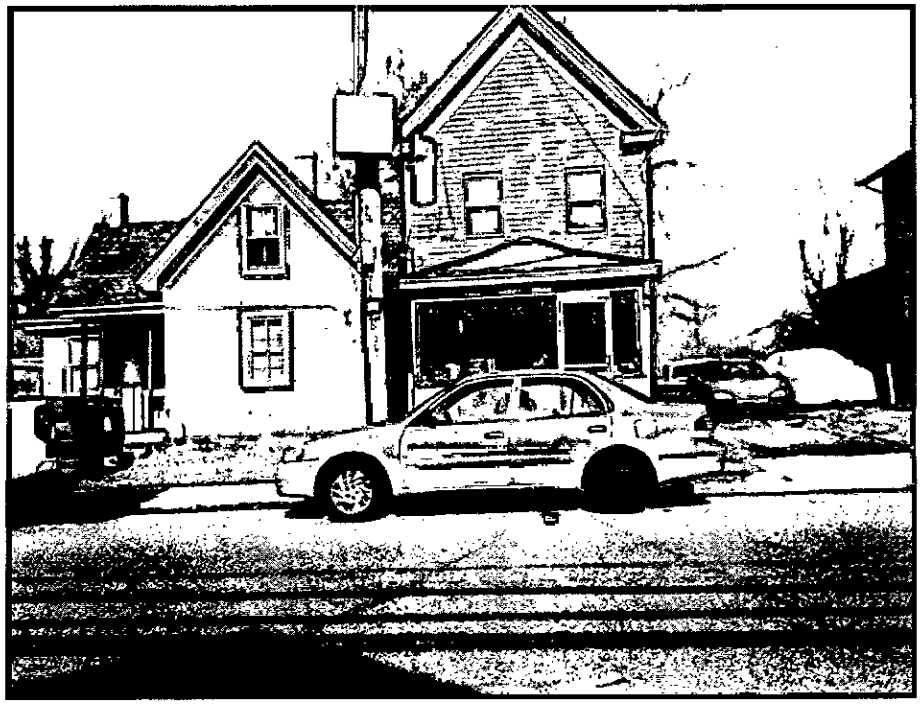
Maryland MVA registration plate number: 3AK5680

13-0579TJS - 13-0584TJS

2000 Gold Chevy Tahoe; with VIN: 1GNEK13T5YJ103097, bearing

Maryland MVA registration plate number: 2AW1295

13-0579TJS – 13-0584TJS



The Premises, known as 647 High Street, Cambridge, Maryland 21613, is described as a two story White siding house with a screened front porch. It has the numbers "647," in White letters with Black background above the screen door.

13-0579TJS – 13-0584TJS

2000 Gray Toyota Corolla, with VIN: 1NXBR12E3YZ403371, bearing

Maryland MVA: 1AN6236 (Actual Vehicle)

13-0579TJS — 13-0584TJS

1998 Lincoln Continental, with VIN: 1LNFM97V6WY664345; bearing

Maryland MVA registration plate number: 1AZ4654

(Photo is for familiarization only; photo of actual car being obtained)

Attachment B

Items To Be Seized

A. Description of items to be seized

ITEMS TO BE SEIZED:

a. Records, (maintained in all forms, including handwritten, typed, computer-generated, floppy disc, readable-writeable compact disc, computer paper, magnetic tape, microfilm or other medium including desktop and laptop computers with internal and/or external hard drives, zip drives, and other hardware, including scanners, necessary to access or to print such files):

1. social security cards both genuine and counterfeit, client lists (including lists of social security numbers, names, addresses and telephone numbers), address and/or telephone notebooks and papers, immigration documents both genuine and counterfeit, passports, and U.S. issued visas both genuine and counterfeit, licenses, immigration document producing materials including ink stamps and stamping materials, computer scanned templates, fraudulent identification documents, photographic equipment, photographs, identification making equipment or items, scanners, document producing software, envelopes bearing the return address of the Social Security Administration, SS-5 receipts, SS-5 applications, correspondence, memos, handwritten notes, and any document or record relating to the Social Security Administration, Immigration and Naturalization Service, and agencies within the Department of Homeland Security, including but not limited to U.S. Citizenship and Immigration Services;

2. credit cards, credit card records including monthly statements, ledgers, and receipts, and bank account statements, financial account records, checkbooks, checkbook ledgers, large sums of money, and other bank records such as passbooks and accounts receivable/payable ledgers; and c) and all documents and keys or other modes of access to safes, cabinets, lock boxes, storage boxes or containers, locked or unlocked, containing the items listed in a) and b) above;

b. Any computer/cellular phone/PDA/cameras used to facilitate the above-listed violations and forensic copies thereof.

c. With respect to any digital devices falling within the scope of the foregoing search categories, or any digital devices containing evidence falling within the scope of the foregoing search categories, records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show the actual user(s) of the digital device during the time period between October of 2011 and the present.

d. As used above, the terms records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form, including in digital form on any digital device and any forensic copies thereof. As used both above and below, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes used to store digital data (excluding analog tapes such as VHS), and memory chips; and security devices.

e. In searching for digital devices and in searching digital data stored on digital devices, law enforcement personnel executing this search warrant will employ the following procedure:

i. Law enforcement personnel or other individuals assisting law enforcement personnel will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The team searching the digital device(s) shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 60 day period from the date of execution of the warrant.

ii. The team searching the digital devices will do so only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

aa. The team may subject all of the data contained in the digital device or the forensic copy capable of containing items to be seized as specified in this warrant to the protocols to determine whether the digital device and any data falls within the items to be seized as set forth herein. The team searching the digital device may also search for and attempt to recover "deleted," "hidden" or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized as set forth herein.

bb. These search protocols also may include the use of tools to exclude normal operating system files that do not need to be searched.

iii. When searching a digital device pursuant to the specific search protocols selected, the team searching the digital device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

iv. If the team searching a digital device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of Court, and shall make and retain notes detailing how the

contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

v. At the conclusion of the search of the digital devices as set forth in subparagraph (a) above, any digital device determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the government until further order of court or one year after the conclusion of the criminal case/investigation.

vi. At the conclusion of the search of the digital devices as set forth in subparagraph (a) above, the government shall retain, for purposes of authenticity and later challenge and review by the defense in any criminal case, all of the digital data on any digital device found to contain digital data falling within the scope of the items to be seized.

vii. Notwithstanding the above, after the completion of the search of the digital devices as set forth in subparagraph (a) above, the government shall not search for digital data on any retained digital devices absent further order of court.

viii. If the team determines a digital device is not an instrumentality of any offense under investigation and does not contain data falling within the list of items to be seized, the team shall return the device as soon as is practicable.

f. In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items, subject to the procedures set forth above:

i. Any digital device capable of being used to commit, further or store evidence of the offense listed above;

ii. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;

v. Any applications, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

13-0579TJS - 13-0584TJS

ii. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.

g. The special procedures relating to digital media found in this warrant govern only the search of digital media pursuant to the authority conferred by this warrant and do not apply to any search of digital media pursuant to any other court order.